Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	

COMMENTS OF YOUMAIL, INC.

YouMail, Inc. ("YouMail"),[1] through counsel, respectfully submits its comments in response to the Federal Communications Commission's ("Commission" or "FCC") Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97.[2]

I. INTRODUCTION AND BACKGROUND

The Commission proposes additional regulations on gateway providers to combat robocalls coming from abroad, changes to the information filed in the FCC's robocall call mitigation database ("RMD") by both gateway providers and other entities, and clarification of voice service providers' ("VSPs") obligations concerning calls to and from Public Safety Answer Points ("PSAPs").

Today, gateway providers bringing foreign calls into the United States must pass along "preexisting authenticated caller ID information unaltered, participate in traceback efforts, and take

[1] YouMail provides security-first, cloud-based communication services for mobile phones. Its free app-based service uses sophisticated, patented technology to block robocalls and phishing messages, protecting users from spam, identity theft, stalkers, and corporate fraud. YouMail's premium call management services provide virtual receptionist and virtual number services, and are designed for people who use their mobile phone for business. These services help customers unify virtual numbers with their mobile number, handle high volumes of mobile calls, and provide personalized answering experiences for their callers. YouMail's communications platform handles over a billion calls per year for over 10 million users, who range from everyday consumers to sole proprietors to the CEOs of the largest companies in America. YouMail is privately funded and based in Irvine, California.

[2] *Advanced Methods to Target and Eliminate Unlawful Robocalls and Call Authentication Trust Anchor*, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 and Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, FCC 21-105, 86 Fed. Reg. 59084 (Oct. 26, 2021) ("*FNPRM*").

steps to effectively mitigate illegal traffic when notified of such traffic by the Commission."[3] Under current Commission rules, gateway providers essentially are treated like intermediate carriers. The latter, however, are not required to apply STIR/SHAKEN authentication to traffic so long as they cooperatively participate in call traceback efforts. Intermediate carriers are also not required to engage in robocall mitigation practices.[4]

Foreign VSPs are prohibited from spoofing Caller ID information with "bad" intent.[5] While foreign VSPs not in the FCC's RMD by September 28, 2021 are having their calls blocked, they can avoid this safeguard by routing calls through a foreign intermediate provider before hitting the gateway provider.[6] This alternative routing through foreign intermediate providers also makes it more difficult to locate foreign VSPs with existing traceback methodologies.[7]

The Commission notes that the largest source of robocalls is from foreign VSPs using NANP resources and that the only way for these calls to enter the United States is through "a gateway provider that is unwilling or unable to block that traffic."[8] In response to these findings, the FCC asks several questions and proposes various rule changes pursuant to this FNPRM.

II. A CAREFUL BALANCE BETWEEN ALLOWING MARKETS TO FUNCTION AND STOPPING ROBOCALLS

The Commission, in evaluating proposed rules for gateway providers (and, hence, foreign traffic coming to the United States), must draw a careful balance between allowing markets to function and stopping robocalls. Foreign providers using NANP resources are a major (if not, the primary)

---

[3] *Id.* at ¶ 22.

[4] *Id.* at ¶ 24.

[5] 47 U.S.C. § 227(e)(1).

[6] *FNPRM* at ¶ 24. For example, assume a foreign VSP, Carrier A, does not route a U.S.-bound call with a NANP number in the Caller ID field directly to U.S gateway Carrier B. Rather, Carrier A routes the call through a foreign intermediate Carrier C, which, in turn, routes the call to Carrier B in the United States. Absent more information, Carrier B has no knowledge that Carrier A originated the U.S.-bound call with a North American Numbering Plan ("NANP") number in the Caller ID field.

[7] *Id.*

[8] *Id.* at ¶ 27.

source of robocalls. These include unlawful and fraudulent calls designed to swindle American consumers and small businesses or damage larger businesses by misappropriating their good names. The Commission has already determined, at least by default, that overseas traffic bound for the United States often can display a NANP number in the Caller ID field.[1] This practice, in turn, suggests the call is being originated by a U.S.-based entity that encourages the called party to answer the call. While many of these calls are illegal or undesirable robocalls, many others are also lawful, legitimate, and desirable. Indeed, there is a large market for delivering lawful, legitimate, and yes, even desirable, robocalls (autodialed) from overseas to the United States.

The Commission must, therefore, find a reasonable balance that will enable VSPs to use analytics and appropriate "know your customer" ("KYC") practices to increase the likelihood that robocalls can be separated from legitimate calls, maximizing the odds that only bad calls will be blocked and all legitimate calls completed.

III. THE COMMISSION SHOULD ADOPT A "SAFE HARBOR" FOR SERVICE PROVIDERS PROPERLY ADDRESSING INCOMING FOREIGN CALLS USING NANP RESOURCES

The *FNPRM* includes a discussion of the various safe harbors the Commission created to incentivize actions and behaviors by VSPs to reduce robocalls.[9] In essence, a safe harbor defines behavior or actions desired by a regulatory agency to achieve a public purpose and provides an incentive for persons to engage in this behavior or to take this action by the agency's "promise" not to sanction or, sometimes, even to investigate the person who has engaged in the desired behavior or performed the desired actions.

---

[1] Today, any available NANP telephone number can be used by a foreign-based business for its outbound number. Thus, absent more information, consumers cannot tell whether the calling party is based in the United States or in a different nation. With its exclusive authority over telephone numbers in the United States, pursuant to 47 U.S.C. § 251(e)(1), the Commission could propose new rules that would require the NANP administrator to designate a new Area Code for exclusive use in foreign locations. Over time, consumers would learn to recognize the Area Code and its purpose. To stimulate consumers to answer calls from these numbers, VSPs, most especially gateway providers, would have an even stronger incentive to stop robocalling from these numbers.

[9] *FNPRM* at ¶¶ 20-21.

Based on its extensive experience in robocall analytics and work with many VSPs and other entities identifying and blocking robocalls, YouMail has concluded that efficient functioning of markets depends on the FCC's adoption of a "safe harbor" that will ensure compliance with FCC rules without undue damage to the market for the delivery of foreign calls to the United States. This should include legitimate calls containing NANP numbers in the Caller ID field. Qualification for such a safe harbor would also constitute a "clear manifestation" of a VSP's intention to comply with other statutes, rules and industry standards.[10]

A. Service Providers Are Governed by Multiple Agency Regulations—The FTC's "Known or Had Reason to Know" Standard

The worry for VSPs is greater than just FCC rules and orders. For example, a party can be liable under Section 5 the Federal Trade Act ("FTA")[11] and the rules promulgated by the FTC under that law, such as the Telemarketing Sales Rule ("TSR"),[12] when the party knows or should have known that the action at issue was unlawful. This was the case in *U.S. v. Dish Network LLC*,[13] where the court of appeals upheld a violation of the TSR on the part of a satellite TV company where its agents made unlawful calls because the principal knew or had reason to know (knowledge fairly implied) that the actions were unlawful.[14] The standard "knew or should have known" based on the facts is an appropriate standard for the FCC to use as well. Indeed, the Commission has done so in several Telephone Consumer Protection Act ("TCPA") cases.[15]

---

[10] For example, the anti-robocall efforts of the Federal Trade Commission ("FTC") and the enforcement of state consumer protection laws by the several state attorneys general ("AGs"), as well as private suits under the TCPA and related laws.

[11] 15 U.S.C. § 45(m).

[12] 16 C.F.R., Part 310.

[13] *U.S. v. Dish Network LLC*, 256 F.Supp.3d 810 (C.D. Ill. 2017), *aff'd*, 954 F.3d 970 (7th Cir. 2020).

[14] *Dish Network LLC*, 954 F.3d at 978 (citing *Jerman v. Carlisle, McNellie, Rini, Kramer & Ulrich LPA,* 559 U.S. 573, 583–84 (2010)).

[15] *See FAX.COM, Inc.*, 19 FCC Rcd. 748, at ¶ 11 (2004) (rejecting a fax-blaster's argument that a district court decision (later reversed) concluding the TCPA was unconstitutional should block an FCC enforcement action because 90% of the faxes transmitted by the defendant were made before the district decision was made, thus, the defendant "**knew, or should have known**, that its fax broadcasting activities violated the TCPA and could result in the assessment of a forfeiture" (emphasis added)); *see also John C. Spiller,*

All of these factors provide a strong incentive for all VSPs, except for those that intend to operate in violation of law for as long as they can, to comply with reasonable and understandable rules to curb robocalls, most especially if such compliance delivers safe harbor protection. The question then moves to: What should be required for a VSP to obtain safe harbor protection?

B. Reliance on KYC Alone Will not Work and Could Even Result in More Robocalling

KYC practices are, indeed, an important part of robocall mitigation. We are in the mess we are in—in part—because, for too long, too many providers used a "See-No-Evil, Hear-No-Evil, Speak-No-Evil" approach to robocalls, particularly for overseas calls from foreign-based businesses using NANP resources. Accordingly, the Commission has been correct in demanding VSPs and intermediate providers use reasonable KYC practices. However, the extent of these practices must be based on the actual level of risk. A retail VSP to only residential and small businesses can have a simpler KYC policy than a wholesale provider or a retail provider servicing call centers. Thus, it stands to reason that those who directly serve foreign providers or call centers, especially those using NANP resources, must have the most rigorous KYC policies of all.

---

35 FCC Rcd. 5948, at ¶ 32 (2020) (holding that a company advertising itself as a provider of telemarketing services "**knew or should have known** about the TCPA requirements and restrictions that govern telemarketing" (emphasis added)); *see also Affordable Enterprises of Arizona, LLC*, 35 FCC Rcd. 12142, at ¶ 22 (2020) (rejecting an argument that the defendant did not know it was displaying numbers which it did not have a right to use, the FCC stated: "To the extent Affordable was not already aware that it was using the numbers of Innocent Customers (again, the evidence shows that Affordable **knew or should have known** as much), its own searches for online complaints put Affordable on notice that it was displaying phone numbers that it no longer had a right to use, as well as numbers it never had the right to use" (emphasis added)); *see also Kenneth Moser dba Marketing Support Systems*, 35 FCC Rcd. 13415, ¶ 18 (2020) (rejecting defendant's argument that he did not know the telephone number he used with robocalls belonged to another entity, the FCC stated: "Moser knew that the phone number he selected for the caller ID had been associated with HomeyTel. And the evidence contradicts Moser's claim that he was not aware that the number still belonged to HomeyTel, which he contends is a 'defunct' business entity. First, Moser **knew or should have known** that the number was still assigned and in service because he stated that his calls went to voicemail when he called that number. Voicemail requires a phone line to be active and in service; thus, if Moser tested the number to see if it was active, as he claims to have done, the voicemail response made it obvious that the line was in service" (emphasis added) (internal footnotes omitted)).

However, KYC must be a scalpel and not an axe. The regulatory imposition of extreme pre-contracting KYC obligations on gateway providers, for example, will cause disruption of commerce and favor carriers that have less robust KYC practices in place. Bad traffic will naturally gravitate to gateway providers with the weakest KYC programs. Indeed, the Commission should expect "See-No-Evil, Hear-No-Evil, Speak-No-Evil" operators to form, scam the market and disappear before the FCC, FTC, or other law enforcement agencies can identify and stop them.

YouMail submits that the better approach is to create a safe harbor that incorporates targeted/focused KYC that can occur AFTER contracting, but before beginning service to the customer or foreign VSP. To qualify for safe harbor protection, domestic VSPs will be expected to build protections into their contracts[16] that enable them to shut down specific telephone numbers that bear indicia of robocalls and fraud (see below). There is no need to shut down all traffic from that source when more targeted action can be taken to address the bad traffic.

As noted above, gateway providers are at risk of enforcement from not just the FCC, but also the FTC and state attorneys general, not to mention the plaintiff's bar and potential slew of class action lawsuits. With these negative incentives, gateway providers have strong economic reasons to identify and shut down bad traffic quickly. As such, YouMail advocates for the creation of an FCC "safe harbor", one that relies on market forces working in harmony with the regulatory scheme, in order to reduce bad traffic, including fraudulent calls.

C. Use of Call Analytics is the Key to Preventing Robocalls

YouMail submits that the universal use of appropriate call analytics is the key to robocall prevention. YouMail makes this statement based on years of experience working to identify and stop

[16] For example, a prudent gateway provider would likely include robocall performance standards (*e.g.*, fewer than X% of traffic bears the indicia of robocalls over Y period of time); prior consent to shut down individual telephone numbers that carry robocall indicia; restrictions against permitting sources of bad traffic to "switch to clean numbers;" and a requirement to post performance bonds to ensure compliance with anti-robocall rules and standards.

robocalls and development of a proprietary call analytics system. With the consent of YouMail's 10 million customers, which range from individual consumers to small-to-mid-sized businesses and nonprofits to enterprise customers as well as carriers and other VSPs, YouMail's technology answers more than one billion telephone calls per year. That is one billion datapoints that are added annually to YouMail's already robust call analytics system. YouMail also uses its data to power the Robocall Index™, the nation's definitive source on telephone network activity and attacks. YouMail's analytics system, therefore, knows the hallmarks/indicia of robocalls, including fraudulent calls, and possesses an ability to, with strong certitude, classify incoming calls as spam or fraud in almost-real-time.[17]

Users of YouMail's analytics can generally identify potential robocalls, including fraudulent calls, quickly and, sometimes, in real time (for example, a high number of calls from the same or similar Caller ID or Caller ID pattern is a hallmark of robocalls). That enables quick investigation or verification. Such knowledge allows the VSP to take meaningful corrective measures within a reasonable period of time, including by shutting down calls based on the call characteristics or, if needed, the source of the calls. This can be done either independently or within the framework of the US Telecom traceback process.

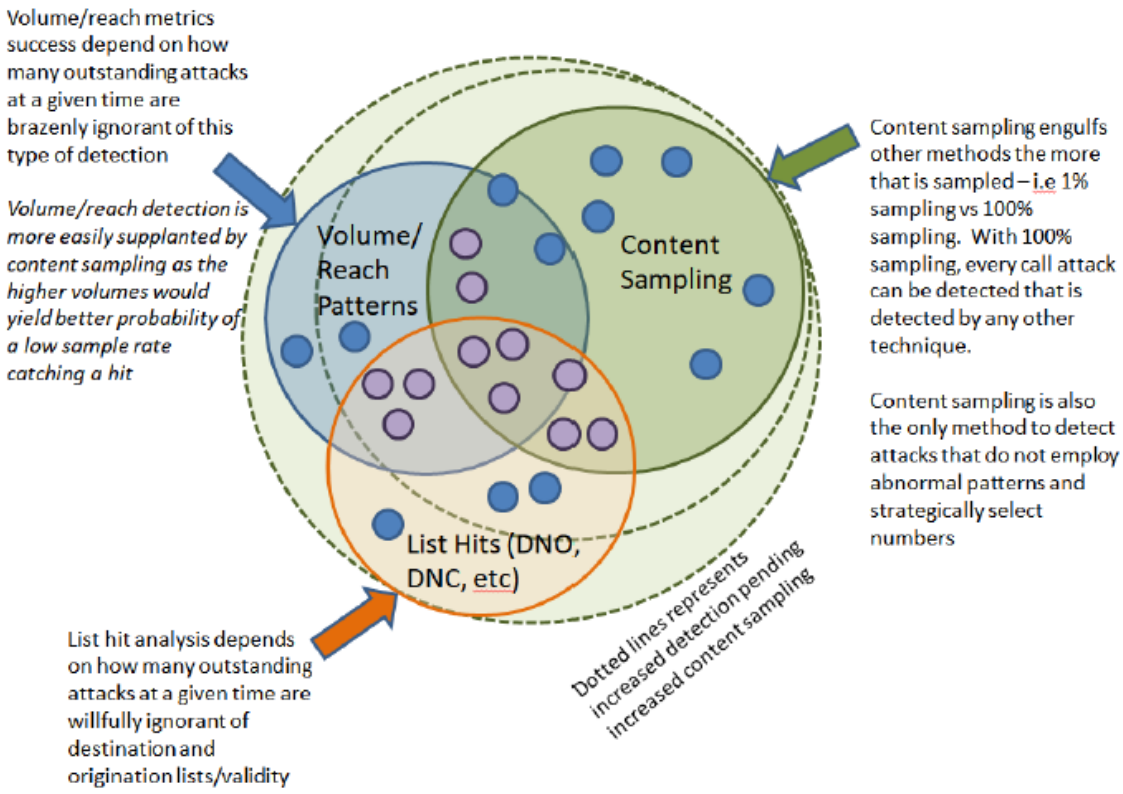
How does fraudulent call/robocall identification work? As Figure 1 illustrates, while there are many different types of analytics that can identify likely robocalls, each has some significant limitations that, in turn, can be overcome by a sophisticated robocaller and/or calling platform. Only 100% content sampling can catch calls that are not identified by other types of call analytics.

YouMail's basic consumer service automatically compares the caller ID against its library of millions of "bad" numbers. If there is a match, YouMail instantly sends the call to a greeting that says, "this number is not in service." YouMail's customers can elect to answer their phone or have YouMail answer it. When YouMail answers calls, the call is recorded, with the customer's prior consent. When

[17] Of course, there are also VSP internal and third-party analytic systems. In short, there are call analytics options already available on the market that could be implemented by most, if not all, VSPs.

these calls involve a robocall campaign (be it unlawful telemarketing because the customer's number is registered on the national "Do-Not-Call" ("DNC") list or outright fraud), details of the campaign message are then available to identify robocall campaigns without reference to the calling numbers. As the number of YouMail customers called increases and the same message or pattern appears, similar calls can be quarantined and not delivered to customers. For example, fraudulent calls purportedly coming from the Internal Revenue Service or the Social Security Administration will never be delivered to YouMail's customers.

Figure 1



As noted earlier, because of the known risk of foreign traffic displaying NANP numbers in the Caller ID field, all gateway providers should bear a burden to analyze all of the traffic flowing through their networks from overseas either through internal analytics, third-party analytics, or a combination

thereof. The economic choice for all but the largest gateway operators is to consider third-party analytics that can greatly improve the quality of their overseas traffic.

Based on YouMail's experience, for any gateway provider with significant call volumes, the majority of those calls should have durations of more than 20 seconds each: the caller either (1) wants the called party to answer or (2) can be expected to leave a voicemail message, as the goal of legitimate calls is to make contact with the called party. And that effort to make contact generally takes at least 20 seconds. Yet, YouMail's data show that, for some call sources, 50%, 90%, or even 99% of calls last a mere five to ten seconds. This is not enough time for the called party to answer or for the calling party to leave a voicemail message.[18] High volumes of short duration calls are not indicia of bona fide, high value communication attempts. Rather, they are indicia of robocalls that plague consumers and degrade the overall phone network.

YouMail has records of call data subpoenaed by law enforcement or parties to civil litigation where the majority of calls were zero seconds in length; clearly robocalls. The same source also contains, for example, large volumes of "neighborhood spoofing" calls, *i.e.*, matching the called party's NPA-NXX where up to 90% of calls are less than five seconds in duration. These are the types of calls that should be blocked.

While many analytics systems analyze short-duration calls after they occur, other analytic systems, including YouMail's, build short-call analysis into the call delivery path on an affordable basis,[19] thus, providing real-time analysis. That, in turn, will enable gateway providers to shut down bad telephone numbers and, when needed, overseas customers, quickly.

[18] Bona fide call centers tend to limit the number of times that they call consumers to comply with time-of-day restrictions and to avoid irritating the consumer. Thus, the argument that it's reasonable to expect call centers to hang up on unanswered calls multiple times a day to "avoid leaving too many voicemail messages" is disingenuous. Gateway providers can use this business reality to measure their traffic and shut down sources of calls that have excessive "hang-up" patterns with very short call durations.

[19] While there are costs for gateway providers to purchase real-time analysis, the cost of labor to download and review non-real-time data, and take action based thereon, can easily offset the costs for real-time analysis.

But more is often needed. The worst of the bad actors are not stupid, whether they are callers or facilitating providers.[20] Those involved in targeted attacks with an intent to commit fraud or ID theft are willfully ignoring robocall hallmarks identified with analytics today. They also generally avoid the more easily caught violations. Many avoid autodialing numbers on the FTC's national DNC registry or calling from the FCC's Do-Not-Originate ("DNO") list. Some avoid use of spoofed telephone numbers or limit calling volumes per originating number to levels unlikely to be detected by analytics as "abnormal." Yet, they still produce unwanted, illegal and fraudulent calls.

YouMail believes that auditing and analysis of calling patterns needs to be supplemented by research of both public and private information providing evidence that specific call sources are committing harm to the public. This can be done through periodic "content sampling" of robocalls and "complaint boards." This information can be found on numerous robocall registries, such as 800notes, Numberguru and YouMail.

D. The Commission Should Consider Establishing an Index-Based Safe Harbor for Gateway Providers

In order to end the scourge of robocalls from their greatest source—foreign call centers using NANP numbers in the Caller ID field—the Commission should create another safe harbor for gateway providers that hold the key to the door of the American market. However, YouMail believes that this safe harbor must be much more demanding than existing safe harbors while providing gateway carriers with much more protection than existing safe harbors offer.

Performance should be based on an index that would be developed by the Commission that measures how few robocalls, both illegal and unwanted, are delivered by gateway carriers to the United States market. Gateway carriers would be required periodically to measure their performance

[20] *See*, *e.g.,* News Release, "FCC Demands Three More Companies Immediately Stop Facilitating Illegal Robocall Campaigns," Doc. 376789 (rel. October 21, 2021) (citing Duratel, Primo Dialler, and PZ/Illum Telecommunication for transmitting multiple illegal robocall campaigns on their networks).

against the FCC's Index and report it to the Commission. Ideally, the Commission would post the results in a manner similar to how the Federal Aviation Administration ("FAA") does for airline on-time performance, flight delays, and cancellations in its Airline Service Quality Performance System ("ASQP"). The details of the ASQP are found in 14 C.F.R., Part 234 of the U.S. Department of Transportation regulations. The results are available to the public on the FAA's website: https://aspm.faa.gov/.

Gateway providers that meet a minimum standard for a specified period of time should be given safe harbor protection from Commission investigation and sanctions. The Commission should go further and provide broad safe harbor protection for those gateway providers that meet a very high level of performance on a consistent basis. Those are the providers that use both analytics and post-service KYC to allow only a very small number of robocalls, both illegal and unwanted, into the United States.

The Commission has broad authority pursuant to Section 205(a) of the Communications Act of 1934, as amended ("Act"), 47 U.S.C. § 205(a). The Act gives the Commission, after hearing, the authority to determine and prescribe "what classification, regulation, or practice is or will be just, fair, and reasonable, to be thereafter followed." Courts have held that "[t]he … Commission's range of power over the regulated companies extends to . . . charges, practices . . . and is not limited to rates and . . . services."[21] Needless to say, the Commission continues to this day to use its prescriptive authority under Section 205(a).[22]

The Commission well described its authority over VSPs' practices in the *2000 Promotion of Competitive Networks Order:*

> It is well established that the Commission has broad authority to regulate the practices of LECs in connection with their provision of interstate communications services. In addition to the general authority specified in Title I of the Communications Act, Title II

[21] *Carter v. AT&T*, 365 F.2d 486, 496 (5th Cir. 1966) (citing *Ambassador, Inc. v. United States*, 1945, 325 U.S. 317, 323 (1945)), *cert. denied*, 385 U.S. 1008 (1967) (internal quotations omitted).

[22] *See, e.g., Core Comm'ns., Inc.,* WC Docket No. 21-191, FCC 21-109 (rel. Oct. 7, 2021), at ¶ 23.

> provides a specific, substantive framework for the Commission's regulation of such practices. … Finally, Section 205(a) authorizes the Commission "to determine and prescribe ... what ... practice is or will be just, fair, and reasonable" where it is of the opinion that a common carrier practice "is or will be in violation of any of the provisions of this Act." [23]

Given this broad authority (and countless orders where the Commission exercised its authority), it is clear the Commission could prescribe any use of analytics (and other best practices) by a VSP that produces "gold standard" robocall suppression results consistently over a specific time period to constitute just and reasonable practices. So long as the VSP uses analytics and other tools to produce "gold standard" results, the Commission would not investigate or sanction the VSP for violations of FCC robocall rules, regulations and orders, all other things being equal.

Moreover, this prescription can operate as an effective shield against prosecution of the VSP by other entities for conduct that meets the FCC's standard. That result is ensured by the Hobbs Act, 28 U.S.C. § 2342(1). That statute provides that the Courts of Appeal "other than the United States Court of Appeals for the Federal Circuit) [have] exclusive jurisdiction to enjoin, set aside, suspend (in whole or in part), or to determine the validity of—(1) all final orders of the Federal Communication Commission made reviewable by section 402(a) of title 47." Moreover, other courts would be required to follow the FCC's order prescribing the "gold standard" when determining when a VSP met those standards. So long as the Commission adopts "legislative rules" using notice and comment procedures under Administrative Procedure Act, district courts[24] are bound by the Commission's orders.[25]

Such a prescription would then protect those VSPs that take sufficient steps, *i.e.*, that meet the "gold standard," to thwart robocalls of all kinds, thus, benefiting consumers, legitimate marketers, and the public interest. These entities would be protected, as a matter of law, against actions by

---

[23] *Promotion of Competitive Networks*, 15 FCC Rcd. 22983, at ¶ 134 (2000).

[24] Needless to say, state courts cannot negate or fail to follow the legislative rules of the FCC with respect to issues within the Commission's statutory authority.

[25] *PDR Network, LLC v. Carlton & Harris Chiropractic, Inc.*, 159 S. Ct. 2051, 2055–56 (2019), *on remand*, 982 F.3d 258 (4th Cir. 2020).

other federal agencies or officers, state agencies or officers and private party suits. YouMail submits that this incentive would drastically reduce the number of robocalls, most especially from foreign sources using NANP resources.

IV. Conclusion

For the reasons set forth above, YouMail urges the Commission to draw a careful balance between allowing markets to function and stopping robocalls; adopt a "safe harbor" for VSPs properly addressing incoming foreign calls using NANP resources, using analytics and other robocall mitigation tools; and establish an index-based safe harbor for gateway providers. As explained in footnote 9, the Commission should also consider designating unique Area Codes for foreign-based call centers using NANP resources.

Respectfully submitted,
YouMail, Inc.

By /s/ Robert H. Jackson

Robert H. Jackson
Jonathan S. Marashlian

MARASHLIAN & DONAHUE, PLLC
The CommLaw Group
1430 Spring Hill Road, Suite 310
Tysons, VA 22102

Tel: 703-714-1300
E-mail: rhj@CommLawGroup.com
jsm@CommLawGroup.com

December 8, 2021